

Remarks

Claims 1-28 are pending in this application. In a final Office Action mailed August 2, 2007, the Examiner rejected claims 1-28 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,424,717 to Pinder *et al.* ("Pinder") in view of U.S. Patent No. 5,784,095 to Robbins *et al.* ("Robbins"). Applicants respectfully disagree with the Examiner's rejections and request reconsideration in light of the following remarks.

Claim 1 provides a system for multi-stream security processing and distributing digital media streams. The system includes a headend, a network coupled to the headend, and at least one receiver coupled to the network. The headend is configured to generate encrypted digital media streams and download software. The receiver is configured to receive the encrypted digital media streams and downloaded software and to present a decrypted version of the encrypted digital media streams based on the downloaded software. The receiver includes a security processor configured to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams. The security processor stores the downloaded software and securely configures, renews, and re-configures at least one of encryption and decryption by the security processor based on the downloaded software.

Independent claim 11 provides a method of multi-stream security processing and distributing digital media streams. Encrypted digital media streams are generated at a headend. A network is coupled to the headend and receives the encrypted digital media streams. A receiver is coupled to the network, the receiver receiving a software download from the network. The encrypted digital media streams are received at the receiver. A decrypted version of the encrypted digital media streams is presented using the receiver. A security processor in the receiver is re-configured based on the software download to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams. The software download is stored in the security processor.

The Examiner rejected claims 1 and 11 as an obvious combination of Pinder and Robbins. Neither Pinder nor Robbins teach or fairly suggest software downloaded to a security processor from a headend that configures or reconfigures the security processor for encryption or decryption of digital media streams.

The Examiner admitted that Pinder does not disclose Applicants' security processor reconfigured by downloaded software as claimed. Instead, the Examiner offered Robbins, stating as the only support "col. 5, lines 1-6, col. 13, lines 65-67." (Office Action, pg. 3.) The paragraph including the first cited passage is provided below.

The CDC 34 is used to control the settop terminal 112 through commands that initialize and configure the settop terminal 112. The settop terminal 112 incorporates a microprocessor executing a program loaded into an EEPROM (as firmware) for the various levels of services. The CDC 34 can be used to download new releases of settop terminal 112 firmware from the headend 16 when system 10 requirements change or new features are desired. The CDC 34 will service the settop terminal 112 and all of its options. In the preferred embodiment, the control data is sent at a rate of 13,980 bits per second.

Robbins discloses downloading software to implement new "services" or "features." There is no mention of downloading software which configures or reconfigures a security processor for encrypting or decrypting digital media streams.

The second cited passage likewise makes no mention of downloading software which configures or reconfigures a security processor for encrypting or decrypting digital media streams.

The system microprocessor 329 interprets all commands from either the interface keys 323, the navigation keys 325, the remote commander 333, or an IR emitter and responds accordingly. The system microprocessor 329 also receives settop terminal control and channel mapping information broadcast from the system headend 16 by using the CDC 34 from the tuner FM receiver tap 341. This separate control channel updates the system firmware stored in ROM 337 with new releases whenever user subscriptions change or for security. Additionally, program schedule information is periodically downloaded from the system headend 16 to individual subscribers.

Updating firmware for subscription changes or for security does not teach, or fairly suggest, configuring or reconfiguring a processor for encrypting or decrypting digital media streams.

Moreover Pinder, the Examiner's primary reference, actively teaches away from the combination suggested by the Examiner. Pinder discloses encryption and decryption code which is unalterably locked into ROM at the time in which the Digital Home Communication Terminal Secure Element (DHCTSE) is manufactured.

Memory 1207 contains the code executed by microprocessor 1201, the keys, and the entitlement information. In a preferred embodiment, there are two kinds of physical memory in memory 1207: ROM 1219, which is read-only memory whose contents are fixed when DHCTSE 627 is manufactured, and non-volatile memory (NVM) 1209, which can be read and written like normal random-access memory, but which retains its current values when DHCTSE 627 is without power.

* * *

FIG. 13 is a schematic overview of the contents of memory 1207 in DHCTSE 627. The memory is divided into two main parts: read-only storage 1301, which contains code and other information that does not change as a result of the interpretation of EMMs, and NVA storage 1303, which is non-volatile storage that changes as a result of the interpretations of EMMs. RO storage 1301 contains code 1305.

Code 1305 falls into four categories: code 1307 for the encryption, decryption, and authentication operations performed by DHCTSE 627, code for interpreting EMMs 1313, code for interpreting ECMs 1321, and code for handling other CA messages such as the FPM and the GBAM.

(Pinder, col. 21, ln. 49-col. 22, ln. 12 (emphasis added).)

Neither Pinder nor Robbins, alone or in combination, teaches or fairly suggests Applicants' security processor that is configured or reconfigured from software downloaded to the security processor to provide encryption or decryption processing of digital media streams. Claims 1 and 11 are patentable over Pinder and Robbins. Claims 2-10 and 12-19, which depend from claims 1 and 11, respectively, are therefore also patentable.

Independent claim 20 provides a security processor configured to provide at least one of simultaneous multiple media stream decryption and encryption processing. The security processor includes a controller operative to be programmed through authenticated firmware downloads from a headend, each firmware download operative to modify media stream processing by the security processor. A memory stores the downloaded firmware. A

plurality of digital stream encryption/decryption engines are selectively coupled by the controller for simultaneous operation in response to a predetermined security configuration downloaded to the controller.

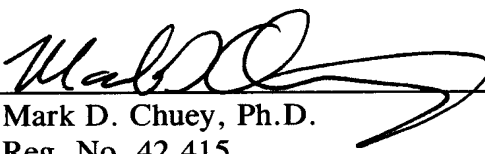
As before, the Examiner relied on a combination of Pinder and Robbins to reject claim 20. The Examiner admitted that Pinder does not disclose downloading firmware for modifying media stream processing to a security processor controller programmed through authenticated such firmware downloads from a headend. Once again, the Examiner relied on Robbins' disclosure at "col. 5, lines 1-6; col. 13, lines 65-67." (Office Action, pg. 4.) As provided above, neither Robbins nor Pinder teach or fairly suggest the claimed firmware download. Claim 20 is patentable over any combination of Pinder and Robbins. Claims 21-28, which depend from claim 20, are therefore also patentable.

Claims 1-28 are pending in this application. Applicants believe these claims are patentable and respectfully request that this case be passed to issuance. No fee is believed due by filing this paper. However, if any fee is due, please charge any fee as a result of the filing of this paper to our Deposit Account No. 02-3978.

The Examiner is invited to contact the undersigned to discuss any aspect of this case.

Respectfully submitted,

JAMES W. FAHRNY et al.

By 
Mark D. Chuey, Ph.D.
Reg. No. 42,415
Attorney/Agent for Applicant

Date: September 26, 2007

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351